

Google scholar

elgamal substitution (parallel or serial) encryption

Search

[Advanced Scholar Search](#)

Scholar

Articles and patents

anytime

include citations



Create email alert

Results **31 - 40** of about **111**. (0.29 sec)

### [BOOK] [Digital rights management and code obfuscation](#)

[\[PDF\] from psu.edu](#)

A Sethi, University of Waterloo. Dept. of Combinatorics ... - 2003 - Citeseer

... We will discuss how the MAC is used, later in this chapter. 3.3 Elliptic Curve Cryptography For Elliptic Curve Cryptography (ECC), Microsoft uses the **EIGamal encryption** scheme, and a curve over  $\mathbb{Z}_p$  where  $p$  is the 160-bit prime given below. The curve is defined by ...

[Cited by 1](#) - [Related articles](#) - [View as HTML](#) - [Library Search](#) - [All 12 versions](#)

### [SIGNAL PROCESSING APPARATUS AND METHOD FOR PERFORMING MODULAR MULTIPLICATION IN AN ELECTRONIC DEVICE, AND SMART CARD USING ...](#)

KH Lee, BJ Im, MS Huh - US Patent App. 11/849,880, 2007 - Google Patents

... 14, 2003 and assigned **Serial** No. ... has been adapted as an international standard of these algorithms, DSA (Digital Signature Standard) as a modification of **EIGamal** has been ... Each of the CSAs 120 and 150 is composed of  $(n+4)$  full adders in **parallel**, each of which has a 3 bit ...

[All 2 versions](#)

### [PDF] [Introduction to elliptic curve cryptography](#)

[\[PDF\] from psu.edu](#)

E Oswald - Online at: <http://www.iaik.tu-graz.ac.at/aboutus/> ... - Citeseer

... beginning of public key cryptography there are two major cryptosystems (RSA and **EI-Gamal**) that seem ... Efficient **encryption**/decryption is not so important because these operations are usually done with a ... take a look what is happening to the left side after the **substitution** for  $Y$  ...

[Cited by 10](#) - [Related articles](#) - [View as HTML](#) - [All 12 versions](#)

### [PDF] [SECCODES-Secure Communication Development System](#)

[\[PDF\] from politicaexterna.com](#)

MT Shimanuki - 2003 - biblioteca.politicaexterna.com

... Page 2. Thesis presented to the Faculty of the Division of Graduate Studies of the Technological Institute of Aeronautics in **partial** fulfillment of ... 73 5.5 Reconstructed voice performance using **substitution** operation cipher . . . . . DECODER TXD P11 RXD **SERIAL** 0 P02 FMEN P15 ...

[Related articles](#) - [All 5 versions](#)

### [PDF] [INSTITUTO SUPERIOR TÉCNICO](#)

[\[PDF\] from psu.edu](#)

RFL Joaquim - 2005 - Citeseer

... that is a variation of the **EIGamal encryption** algorithm). The algorithm of ... in this case we use the private key for **encryption** (signing) and the public key for decryption (signature verification), as follows: ... to B. Making a **parallel** with the paper-based world, getting a blind signature ...

[Related articles](#) - [View as HTML](#) - [All 4 versions](#)

[\[PDF\] Note to the Reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. Italicized page numbers indicate illustrations.](#)

[\[PDF\] from wiley.com](#)

L. Adleman - biometrics - media.wiley.com

... asymmetric cryptography, 288 **El Gamal**, 291 elliptic curve, 291–292 keys in, 268–270, 288 ... codes, 262 in cryptography, 262–266 defined, 599 **substitution**, 263–264 transposition, 263 ... 257, 599 CIR (Committed Information Rate) contracts, 87, 600 circuit **encryption**, 305 circuit ...

[View as HTML](#) - [All 3 versions](#)

[Aspects of hardware methodologies for the NTRU public-key cryptosystem](#)

[\[PDF\] from rit.edu](#)

K. Wilhelm - 2008 - ritdml.rit.edu

...  $\alpha a = \beta$  and  $0 \leq a \leq n-1$  • Alternatively,  $a = \log_{\alpha} \beta$  The **ElGamal** cryptosystem is based on the discrete logarithm problem, achieving secu- ...  $e \equiv r * h + m \pmod{q}$  **substitute**  $h \equiv pfq * g \pmod{q}$   $e \equiv r * (pfq * g) + m \pmod{q}$  ... ultra-low application of NTRU **encryption**. ...

[Cited by 3](#) - [Related articles](#) - [View as HTML](#) - [All 2 versions](#)

[Implementation Of Security Within GEN2 Protocol](#)

[\[PDF\] from uta.edu](#)

SK Jagannatha - 2010 - dspace.uta.edu

... Presented to the Faculty of the Graduate School of The University of Texas at Arlington in **Partial** Fulfillment ... This used a simple cryptographic design which does the public key **encryption** of the **serial** numbers in RFID tags with a corresponding private key stored appropri- ...

[Related articles](#) - [View as HTML](#)

[Method and apparatus for enhancing software security and distributing software](#)

SL Chang, J Gosling - US Patent 5,724,425, 1998 - Google Patents

... 5,724,425 1 METHOD AND APPARATUS FOR ENHANCING SOFTWARE SECURITY AND DISTRIBUTING SOFTWARE BACKGROUND OF THE INVENTION 1. Field of the Invention The present invention relates to the use of public key **encryption**, and more particularly, the ...

[Cited by 177](#) - [Related articles](#) - [All 2 versions](#)


[\[PDF\] PUBLIC-KEY CRYPTOGRAPHY NIST Special Publication 800-2](#)

[\[PDF\] from psu.edu](#)

J. Nechvatal - NIST Special Publication, 1991 - Citeseer

... 94 B.4.2 Proposal for a quadratic sieve machine.....95 B.4.3 Massively **parallel** machines.....95 ... Figure 7. The **ElGamal** Signature Algorithm.....51 ... where P is a certain permutation and F is a certain function which combines permutation and **substitution**. ...

[Related articles](#) - [View as HTML](#) - [All 15 versions](#)

 [Create email alert](#)



Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [Next](#)

elgamal substitution (parallel or serial) encryption partial

Search

[Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2010 Google